US Army Corps
of Engineers

Electronic Signature
for
Windows 95/NT

(WinSig)

Users Guide

Corps of Engineers Financial Management System

May 2, 2002

Electronic Signature
For Windows 95/NT
(WinSig)
Users Guide

WINSIG USERS GUIDE

TABLE OF CONTENTS

PAGE

WINSIG USERS GUIDE

1.0 GENERAL

1.1 Introduction.

The Corps of Engineers Financial Management System (CEFMS) provides the capability to electronically sign documents. The electronic signature generated by the system is a replacement for a handwritten signature. An electronic signature provides assurance that an authorized person signed a document and that the document was not altered after it was signed. Hardcopy documents can be altered without detection and handwritten signatures can be forged. With electronic signatures, these alterations will be detected. Electronic Signatures will reduce the amount of paper that must be routed. Documents can be reviewed on screen and signatures verified using the Electronic Signature System (ESS).

An Electronic Signature, or Message Authentication Code (MAC), is a cryptographic checksum calculated by a cryptographic algorithm, based on the Digital Encryption Standard. This algorithm is stored in firmware which resides in the user's PC. The information that must be supplied to the cryptographic module so that a MAC can be generated include:

- A secret key belonging to the person signing or MACing the data. This person is the user.
- A secret key belonging to the person allowing the user to electronically sign data. This person is the Security Administrator (SA).
- The data to be MACed.

Reference the MAC Cross-Reference Guide for a detailed explanation of the MACing procedure.

The secret keys are resident on each SA and user smartcard and in the smartcard database at each Key Translation Center (KTC). A smartcard (also referred to as "token") is similar to a credit card but contains a complete computer resident in chip form. The signing process generates a MAC and an encryption key. Please note that the data is not encrypted. The encryption key is used in the verification process and is not an encrypted form of the data. At any point in time, the MAC may be verified. The verification process ensures that none of the data associated with the MAC has changed. The verification process also requires the secret keys

of an SA and user. The SA and user that request to verify a MAC do not have access to the secret keys of the SA and user which generated the MAC. This is where key translation comes into the Electronic Signature process. The IDs of the SA and user that were used to generate the MAC plus the IDs of the SA and user wishing to verify the MAC along with the original encryption key must be sent to the KTC. If the information received by the KTC is valid, the KTC will generate a verification key based upon the received information and send the verification key back to the SA and user wishing to verify the MAC. The process of generating a verification key is called *key translation*. The verification key, along with the secret keys of the SA and user wishing to verify the MAC and the data are input to the cryptographic module which results in the generation of another MAC. If this new MAC and the original MAC are identical, the data has not changed. Different MACs indicate that the data has changed and the verification fails.

In addition to providing key translation services, the KTC provides the capability to:

- Create User Smartcards
- Create SA Smartcards
- Create District Security Officer (dSO) Smartcards
- Create Central Security Officer (cSO) Smartcards
- Transmit key information between KTCs electronically and on magnetic media

1.2 Explanation of WinSig.

The initial CEFMS electronic signature system was designed and implemented using the UNIX system standard-in and standard-out file descriptors to perform all communications between CEFMS (at the remote host) and the cryptographic module in each user's computer. This design was based on the domination of the DOS operating system, therefore, no other options were readily viable.

Due to technological changes, Microsoft Windows is rapidly becoming the operating system of choice. Microsoft Window's graphical interface and multitasking capabilities make it very appealing to computer users. To keep up with the needs of CEFMS users, the U.S. Army Corps of Engineers (USACE) determined that CEFMS should migrate to the Windows environment. In order to make this transition

possible, the first step is to convert the electronic signature system since it is both DOS-based and terminal dependent. To facilitate this port, the electronic signature system has been rewritten to work in a Windows environment. The new software is called WinSig, and it provides the following benefits:

- Users are no longer bound by the limitations of DOS.
- Electronic signature is no longer dependent on a specific communications medium, therefore, allowing users a choice of terminal emulator. Any terminal emulator that can support CORP220 emulation can be used with WinSig.
- Portability of CEFMS to Windows will be minimal because WinSig already works in Windows. Only the user exit portion (the subsystem that actually talks to the database) will need to be ported from UNIX to Windows.
- The WinSig design makes the port to a database trigger-based electronic signature system easier and less time-consuming.
- WinSig is generic; making it easily integrated into other applications, like travel systems, or e-mail systems.
- Users can see, on their screen, a detailed list of all the data they are signing, and elect whether to sign it or not.
- Signature failure resolution is performed interactively, and the users can elect to re-sign a document while still in CEFMS.
- Communications hashing is no longer needed, since the users sign data visible on their screen. Elimination of communications hashing reduces the number of UNIX processes that were required and the increased communication traffic for KTC access.
- There is no longer a need for standalone resigning programs.

1.3 Hardware/Software Requirements.

The basic computer software and hardware required to run and use the WinSig suite include:

- A PC with one available ISA slot, capable of running Windows 95 or NT. **NOTE:** WinSig will not work on a Macintosh. WinSig may be used with a notebook computer with the Signet device, when the Signet driver for WinSig becomes available. If using the Signet device, one serial port is needed.

- Windows 95 or NT.

- Capability to access the CEFMS database via a telnet connection. Users wishing to use WinSig with a modem will need to use the Windows Dial-up Networking software, or a similar product.

- Cryptographic module and smartcard reader.

- WinSig.

- Activated Smartcard and personal identification number (PIN) for same.

- Users who will not be using the CEFMS electronic signature capabilities will still need to run WinSig with the NoBoard package, in order to be able to print and transfer files.

1.4 Installation Instructions.

WinSig is currently composed of three separate pieces of software: WinSig itself, the CEFMS package for WinSig, and the NoBoard package for WinSig. Use the following to determine what you need:

- All users need WinSig
- Users with a cryptographic module need the “CEFMS package for WinSig”:
- Users without a cryptographic module need the “NoBoard package for WinSig”

To obtain the software, point your web browser to http://www.esig.com/cefms.html, and follow the download instructions there. A copy of the Esig web page is provided on the following page.

First time visit? Check in here and find out a little about the company that can provide security so strong even the government trusts it.	**CEFMS esig web page** A page just for the U.S. Army Corps of Engineers CEFMS users. Find out more about the system you use daily, including error codes, system docs, and current downloads.
Why use esig? A electronic security system provides not only state of the art encryption, but integrity for your data, as well.	**Electronic Signatures explained** Find out the skinny on just *what* one of those MAC things is
Key Management At the heart of the esig system is the key translation center	
Guided tour A walkthrough of the entire signature process, from generation to verification, and beyond.	**Esig Applications** Esig: In more places than you might expect.

It is best to download the software to a temporary location on your PC. When you have downloaded the software you need, you are ready to install.
NOTE: When installing the software on a new PC, WinSig must always be the first software installed, because the other packages install themselves relative to the WinSig installation directory.

Each piece of the WinSig suite is in a single self-extracting executable. To begin the installation process, uncompress the executable by running it. Uncompressing the file will create a group of files in the download directory. To begin the installation, run the setup program ("SETUP.EXE") created during the extraction. This will start an InstallShield setup. Please follow the instructions given in the setup process. It is recommended that only advanced users modify any of the default settings in the Setup process. At the end of the Setup process, a prompt to

“Launch program file” is displayed. *Always* select the box next to this prompt before exiting the Setup program.

When finished with the Setup processes for all the software you need, run the WinSig Package Manager (found on the Start menu). In the Package Manager, select the appropriate package for use by checking the box next to its name in the “Available packages” list. *WinSig will not use a package unless it is selected for use and is configured properly.*

1.4.1 WinSig 2.0.1 Full Installation.

This section provides guidelines for the installation and configuration of WinSig 2.

Download and save the ws2install.exe file somewhere on your PC. Installers may wish to burn the executable to a CD to save time installing on several workstations.
Run ws2install.exe. If you are running on Windows NT or 2000, you must have administrator privileges or the installer will not run.
You'll be presented with three options:

- Use existing WinSig 1.2.1 KTC settings
- Install Esig package
- Configure WinSig upon completion

You are also given the option of selecting where you want WinSig 2 installed.
All three boxes are checked initially, and the default installation location is C:\CEFMS\WINSIG. Make the choices you want (the defaults are strongly recommended for most users), and click the 'Ok' button. **Note: Users needing electronic signature capabilities *must* have the 'Esig' package installed.**
After the installation is complete, the WinSig 2-package manager will be started so you can configure WinSig, if you chose to have the installer start it. The package manager should look familiar. There will be at least one package listed (the 'basic' package, which is required by **all users**) and possibly two (the 'Esig' package is required by users who have electronic signature hardware installed). Two new checkboxes on the package manager control new functionality of the WinSig software. The first, "Force WinSig to front when active" controls how rigorously WinSig tries to put itself on top of other applications. This box is checked by default, and for the vast majority of PCs should remain checked. **Note: PCs used to print checks or perform electronic file transfers (EFT)s within CEFMS *must* uncheck this box or WinChecks/WinEFT will *not* function properly.** The second box, "Start/restart WinSig on exit" should be checked if you want the package manager to kill and restart or start WinSig 2 when you are exiting the package manager.

Configuring the Basic Package

The Basic Package is the heart of WinSig, and provides all non-Esig-related functionality, like printing, file transfers, and the ability to spawn local applications from a remote system. It is essential to WinSig, and WinSig will not work correctly if it is improperly configured.

WinSig creates internal log files for debugging, and the first area in the Basic Package configuration lets you set where you want these files to go. This location defaults to the installation location of WinSig, and it is recommended that you leave it set to that value. **Note: On Windows NT and 2000, the path to the debug log files must be given all access to all users.** Primary and secondary KTC entries tell WinSig where to go for user/smartcard registration, as well as for key translations in electronic signature verifications. It is important that these be correctly entered. If you take the default installation, the KTC entries will automatically populate (assuming WinSig 1.2.1 was previously installed). If your CEFMS machine name starts with "wpc", your primary KTC is tk3.usace.army.mil and your secondary KTC is tk4.usace.army.mil. If your CEFMS machine name starts with "cpc", your primary KTC is tk4.usace.army.mil and your secondary is tk3.usace.army.mil. The CEAP ID, (which is the ID that looks like 'u4rmfxzy' or 'e3im9kcc') for the primary user of this computer, must be entered in the appropriate box, and if you would like WinSig to manually register this user whenever WinSig loads, make sure the "Auto-register user when package loads" box is checked.

Configuring the Esig Package

The Esig Package performs all electronic signature functions required for CEFMS users with smartcards. For it to function properly, it must be properly configured. The cryptographic module Dynamic Link Library (DLL) location tells where the hardware driver software is loaded, and defaults to point to the location where WinSig installed its driver. Should you require another driver, refer to the maker of that driver for assistance. Configuration of the cryptographic module DLL in WinSig 2 is virtually identical to that in previous versions. Make sure you perform the 'search for hardware' option, because if the hardware address is improperly set (it defaults to address 0), WinSig will behave erratically. WinSig must poll the electronic signature hardware regularly to detect if a card has been inserted for smartcard registration. The "check for smartcard insertion every ____ seconds" entry box gives you control over how often WinSig polls the hardware. This value defaults to having WinSig check every second, and can be configured to be any integer value between 1 and 32. **Note: Setting the polling interval to higher numbers can result in WinSig seeming sluggish in registering smartcards.** When performing electronic signature functions within CEFMS, some users may elect to sign large batches of data without having to click the "Sign" button on the "You have received a request to generate an electronic signature"

window. These signature types become "silent" if the user makes this choice, and are listed on the screen displayed when the "Silent MAC generation" button is clicked. That screen can be used to make silent signature windows visible again for specific signature types.

Random Notes for All Users

When WinSig 2 is running, right-clicking on the smartcard icon in the tool tray (most likely at the bottom right of your screen) will bring up a menu with many options. WinSig 2 can be shutdown or restarted from here, or the package manager can be run to reconfigure some aspects of WinSig. WinSig 2 users will notice there is no longer a manual registration icon on the desktop. Manual registration can be performed by looking in the "Basic package" section of the pop-up menu. Under the "Esig package" item in the pop-up (if the Esig package is installed) there is an option which will display the name of the person who SA'd the machine.

Point of Contact

If you need assistance installing or configuring WinSig 2, please contact Fred Anderson at (256) 864-0656. Please designate a single point of contact at each site for calls.

1.4.1.1 WinSig Frequently Asked Questions (FAQ)s.

Question	***Answer***
What exactly is WinSig?	WinSig is software that is essentially a CEFMS device driver that executes on a PC. WinSig provides CEFMS with all the support required on your PC. All Electronic Signature functions, local printing, file transfers, etc., required by CEFMS are performed by WinSig.
Is WinSig a terminal emulator?	No. A terminal emulator must still be used to access CEFMS.
I have heard that WinSig is terminal emulator independent. What does that mean?	Almost any Windows based terminal emulator can now be used for accessing CEFMS. You will no longer be required to use a specific emulator, such as VistaCom for DOS. However, the terminal emulator that you use to access CEFMS must have a VT220 emulation and keyboard re-mapping capability. You will have to re-map the VT220 emulator keys to send the correct ASCII sequence for CEFMS. There are several emulators that already do this.

How much does WinSig cost?	Nothing. WinSig is a Corps of Engineers product and is owned by the Corps.
Do I have to install WinSig right now?	No. But WinSig has to be installed by September 30, 1998 on each PC that accesses CEFMS. We recommend that you begin conversion to WinSig as soon as possible.
With what operating systems will WinSig work?	WinSig will only run under Microsoft Windows 95 and NT 32 bit operating systems.
Where can I get a copy of WinSig?	WinSig may be downloaded from the CEFMS Esig web site at http://www.esig.com/cefms.html. Downloads will be allowed as of April 1, 1998. However, you must request a user name and password to access the download portions of the aforementioned web site. The email address to mail the request to can be obtained from the same web site. Only one download account will be allowed per District or Division.
Will WinSig work with DOS or Windows 3.1 or Windows 3.11?	No.
When using WinSig, do electronic signature functions work the same way as I'm used to?	Electronic signature operations when using WinSig follow all the rules for SA, USER and DSO cards that you are already familiar with.
I have heard that there is an additional operational requirement for electronic signature when using WinSig. Is that true?	Yes. Users must now register their smartcards before using CEFMS for the first time with WinSig.
What is meant by the phrase "registering a smartcard"?	With WinSig, CEFMS must know the IP address of the PC that a user is using to access CEFMS. To provide that information to CEFMS, a user must register their smartcard before accessing CEFMS. Registering a smartcard is accomplished by simply inserting your smartcard into the smartcard reader attached to the PC that you will use to access CEFMS. Nothing will prompt you to do this. When the smartcard is inserted into the card reader a

	window will appear announcing that the smartcard is being registered. If this is the first time that you have registered your card another window will pop up asking that you enter your UNIX logon ID. It is important that you enter the ID correctly. Your UNIX logon ID is also what you may have heard called your "CEAP ID" and is in the form of "u4rmfsrk". Once the ID has been entered, both windows will close in a second or two. When the registration windows have closed, your card has been registered. You are now ready to use CEFMS.
Do I have to register my smartcard every time before I use CEFMS?	That depends. If you are using the same PC and it has the same IP address as when you registered your smartcard, then no, you don't have to register your smartcard again. However, if the IP address of your PC changes (for example, if your site uses dynamic addressing), or if you use a PC with a different IP address, you must register your smartcard before using CEFMS. CEFMS must know the IP address that you are using to access CEFMS. The rule is: If your IP address changes, for whatever reason, you must register your smartcard before accessing CEFMS.
Do I have to enter my UNIX logon ID every time I register my smartcard?	No. You only have to enter your UNIX logon ID when registering a smartcard the first time you use a specific card. When you are issued a new smartcard, you will have to enter your UNIX logon ID the first time you register the smartcard.
I don't use electronic signature when I use CEFMS. The PC that I use does not have an electronic signature board. Will I need to use WinSig?	Absolutely. WinSig performs all PC CEFMS functions, not just Electronic Signature. So each PC that is used to access CEFMS must have WinSig installed.
How do I install WinSig?	WinSig is downloaded in the form of a self-extracting executable. A standard Install Shield installation version (setup.exe) is obtained by running each of the executables in separate directories. WinSig must be installed on each PC that will be used to access CEFMS and is equipped with an electronic signature board. Some configuration of the CEFMS package is required. You will need to know the fully qualified domain names of your site's primary and secondary KTCs. If your CEFMS database resides on a CPC computer, your primary KTC is tk4.usace.army.mil and your secondary KTC is tk3.usace.army.mil. If your CEFMS database resides on a WPC computer your primary KTC is tk3.usace.army.mil and your secondary KTC is tk4.usace.army.mil. You will have to

	specify to the CEFMS package which DLL to use to access your electronic signature board. The DLL's name is "argus300.dll".
I use a laptop computer with a SigNet box to access CEFMS. Will this work with WinSig?	The only electronic signature software that will work with CEFMS after September 30, 1998 is WinSig. WinSig does not provide any device interface to the Signet box because Signet is a proprietary device. However, it is our understanding that the company that sells SigNet is developing a DLL for WinSig. To use SigNet with WinSig will require that that DLL be specified when configuring the CEFMS package for WinSig. You should contact the sellers of SigNet for further information regarding this issue.
Can WinSig and the CEFMS and NoBoard packages be installed from a network drive?	Yes.
Does WinSig allow for network installations?	Yes. WinSig can be installed in such a manner that all common files can reside on a network drive and all unique files reside on a local drive.
Will WinSig function properly if a firewall is installed on our LAN?	Depends. Ports 2400 through 2405 must be unblocked and allow socket connections from the UNIX platform where CEFMS executes back to each PC on your LAN that uses WinSig. Additionally, ports 2198 and 2199 must be open for smartcard registration purposes.
Is it true that WinSig will have electronic signature failure resolution capability?	Yes, indeed. WinSig will tell you exactly what data components changed and their former and current values.

I have heard that WinSig has the capability to re-sign documents, is that true?	Most definitely. WinSig has the functionality to allow for the re-signing (MACing) of documents that have had an electronic signature failure.
What about when I need to re-sign many documents because of running a script?	CEFMS has the capability to re-sign many documents at once without the need of running a stand-alone program like the old ReMAC program. Access the ReMAC option of CEFMS.
I have had some problems printing with WinSig. I've tried different terminal emulators and that doesn't seem to help. What's going on?	First of all, the terminal emulator that you use has nothing to do with printing when using WinSig. All CEFMS functions that are performed on your PC are performed by WinSig, NOT the terminal emulator. WinSig was designed to print documents sent from CEFMS using the Windows 95 or NT print manager/spooler. If you encounter printing problems, report them to the CEFMS hotline.
I have tried to use lprint to print some files and that doesn't work. What can I do to make it work?	Nothing. Lprint *will not* work with WinSig. WinSig uses a UNIX counterpart called WinPrint to perform printing functions. Trying to print files from the UNIX command line using WinPrint should work at your location, but might not with certain printers, because WinPrint was designed to print forms and reports when invoked by CEFMS, not when invoked from the UNIX command line.
I've heard that WinSig doesn't work with routers that use Network Address Translation. Is this true?	Indeed it is. For registration to work properly, the WinSig registries *must* know the true IP address where you are located. Since NAT prevents this, WinSig and CEFMS stop working properly.
Will WinSig work with my firewall?	Yes, if you unblock incoming ports 2400-2407 and outgoing ports 2198 and 2199.

1.5 Instructions on Using WinSig Features.

1.5.1 Starting WinSig.

The WinSig executable is located in the directory where you installed WinSig. If you took the installation defaults, that directory is C:\CEFMS\WINSIG. The WinSig executable is WINSIG.EXE. Additionally, if you took the installation defaults, a link to WinSig should also be in your computer's Startup group, thereby starting WinSig each time you boot your PC.

1.5.2 User and Smartcard Registration.

With WinSig, CEFMS must know the IP address of the PC that a user is using to access CEFMS. To provide that information to CEFMS, a user must register their smartcard before accessing CEFMS. Registering a smartcard is accomplished by simply inserting your smartcard into the smartcard reader attached to the PC that

you will use to access CEFMS. Nothing will prompt you to do this. When the smartcard is inserted into the card reader a window will appear announcing that the smartcard is being registered.

If this is the first time that you have registered your card another window will pop up asking that you enter your UNIX logon ID. It is important that you enter the ID correctly. Your UNIX logon ID is the same as your "CEAP ID" and is in the form of "u4rmfsrk". Once the ID has been entered, both windows will close in a second or two. When the registration widows have closed, your card has been registered.

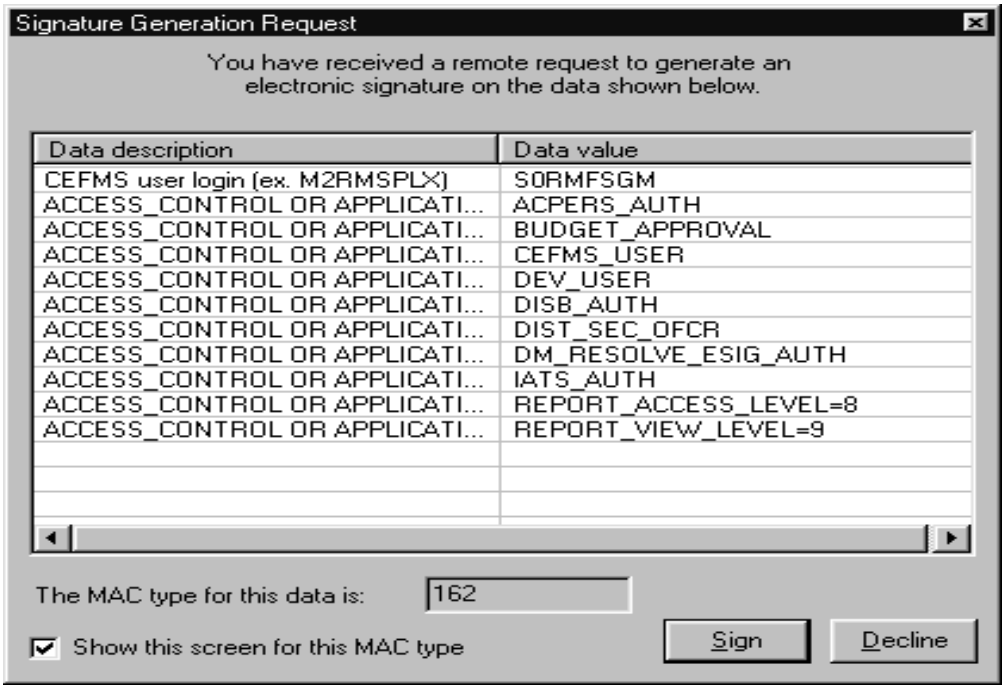
You are now ready to use CEFMS. Once the WinSig registration system knows your ID, you will not be prompted to enter it upon successive registrations.

NOTE: <u>Any time a user's IP address changes, that user needs to re-register to WinSig</u> by inserting his smartcard. Several things can cause an IP address change: moving to another machine, the use of dynamic addressing (DHCP), or a system reboot. *Failure by a user to re-register upon an IP address change will cause WinSig to work improperly.* For users with smartcards, it is recommended that you get into the practice of always inserting your smartcard before you enter CEFMS, to prevent these problems.

If a user tries to enter CEFMS and CEFMS locks up or the user gets into CEFMS with Esig errors, most likely he/she is not registered properly. If a user moves from one machine to another, he/she will need to re-register. If the PC IP address changes (usually due to dynamic addressing); the user must re-register. Several users can share a PC and be registered simultaneously to a PC; however, a user must re-register when using another PC.

The user ID is used by the registry to link a particular CEAP ID with a smartcard (if applicable) and an IP address. WinSig uses ports 2400-2405, and the registry system uses 2198-2199. The following error screen will appear if the user has dm_resolve_esig_auth role. This message is a reminder that you have unresolved Esig data.

1.5.3 <u>Signature Generation</u>. With WinSig, no electronic signature will be generated without the express consent of the user generating the signature. Any time you need to sign some data in CEFMS, you will see a window like the one shown on the page that follows.



All data for a signature is shown in the window, and the scroll bar can be used to navigate the data. To sign the shown data, click the “Yes” button. To decline signing, click “No”. For users signing several documents of the same type over and over (for example, people in disbursing), the check box next to “Show this screen for this MAC type” can be unchecked. If the box is unchecked, the user will not be able to view the data before signing. This process is called *ignoring* a particular MAC type.

NOTE: <u>If you ignore a particular MAC type, the window above will *not* be shown for that MAC. WinSig will assume on ignored MACs that you wish to generate the signature and will sign the received data without prompting you. The user is still responsible for the data being signed. Please do not fail to see the potential ramifications of ignoring a signature type.</u>

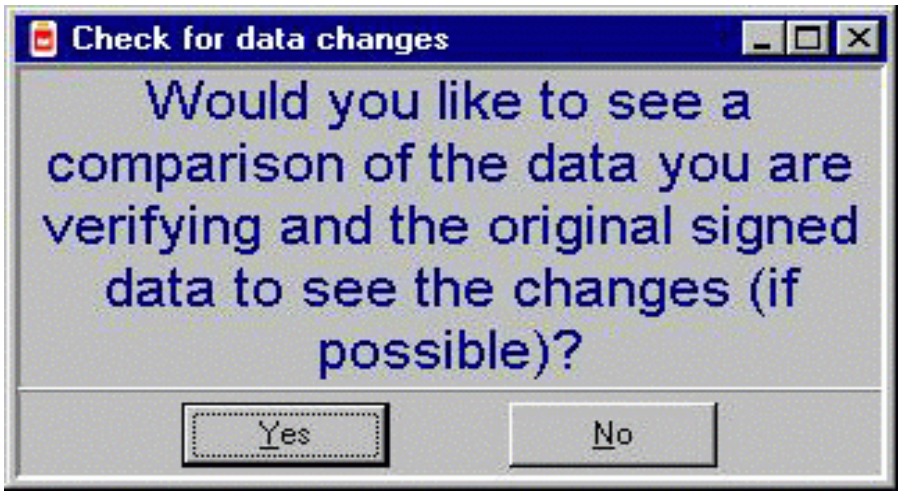
If you want to remove the “ignore” on a particular MAC type:

1. Right-click the smartcard icon in the tool tray when WinSing is running.
2. Select “Configure”.
3. Choose the “Esig package”; click “Configure Package”.
4. Click the “Silent MAC Generation” button.

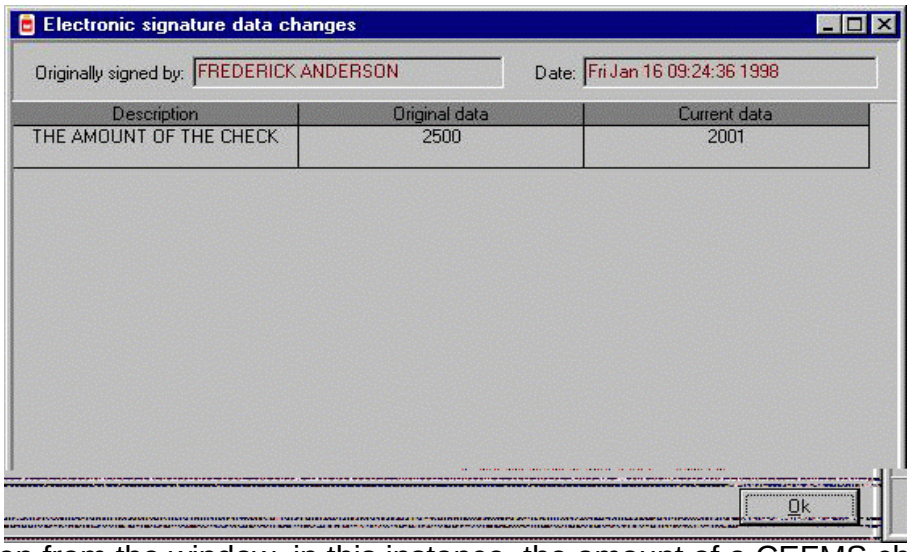
Select the entry from the list to be removed.

1.5.4 Signature Verification.

Signature verification in WinSig, for the most part, is like the signature verification you're used to from the original electronic signature software, with some differences. These differences become apparent when a signature fails. When you have a failure on signature verification, after you are shown an error message, you should see the following window.



WinSig has the ability to research a signature failure and display the changed data for the user as soon as the failure occurs. Clicking the "No" button here dismisses the window and returns control to CEFMS, which in turn displays the error you received. Clicking the "Yes" button will bring up a window similar to the one that follows.



As can be seen from the window, in this instance, the amount of a CEFMS check has been modified from 2500 to 2001. Failure resolution should be considerably

easier now that WinSig can provide this information to the user. Failure resolution is only available if the user signs the document using WinSig and if the log files have not been archived to tape. If the changed data is now incorrect, the site's CEFMS Point of Contact must be contacted in order to get the data changed to the proper value. In most cases, this will require the site to enter a CEFMS customer inquiry. After the user who originally signed the document determines that the data is correct, that user may resign the data.

2.0 REFERENCES

For the resolution of Esig failures, refer to the Electronic Signature Failure Resolution document. For MAC and re-MACing guidelines, refer to the Electronic Signature Message Authentication Code (MAC) Cross-Reference Guide.